54/108Mbps Super G Wireless LAN USB Adapter

WL-U357

User's Manual

Copyright

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes..

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

To assure continued compliance.(example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

Revision

User's Manual for PLANET Wireless USB Adapter

Model: WL-U357

Rev: 1.0 (June. 2005)

Part No. EM-WLU357

TABLE OF CONTENTS

Chapter 1 Introduction

Complying with the IEEE 802.11g standard, WL-U357 provides simple, reliable, high-speed wireless connectivity for both desktop and laptop users. By combining two, state-of-the-art technologies—USB 2.0 and Super G— WL-U357 provides up to 108Mbps data rate in 2.4GHz unlicensed ISM band. Thus makes WL-U357 more suitable for multimedia applications which required more bandwidth

Support of 64, 128 and 152-bit WEP encryption plus WPA (Wi-Fi Protected Access) high-level encryption prevents your wireless communications from unauthorized access and ensures secure data transfer. The WL-U357 is also backward compatible with 802.11b Access Points. Easy installation and Hot-plugging offers full mobility and high availability, making the device a perfect choice for users who are getting tired of running cables or in constant need of wireless access.

1.1 Features

- 2.4GHz ISM band, unlicensed operation
- Wireless connectivity without the hassles and cost of running cables
- IEEE 802.11b/g standard compliant
- USB 2.0 A-type standard connector, compatible with USB 1.1
- Super G mode provides up to 108Mbps data rate
- Utilization of Direct Sequence Spread Spectrum plus OFDM modulation to provide robust, interference-resistant solution in a multi-user environment
- Support of 64/128/152-bit WEP encryption and WPA (Wi-Fi Protected Access) high-level encryption
- Support of Ad-Hoc / Infrastructure mode
- Support of most popular operating systems including Windows 98SE/ME/2000/XP/Server 2003
- Plug-and -Play installation

1.2 Application

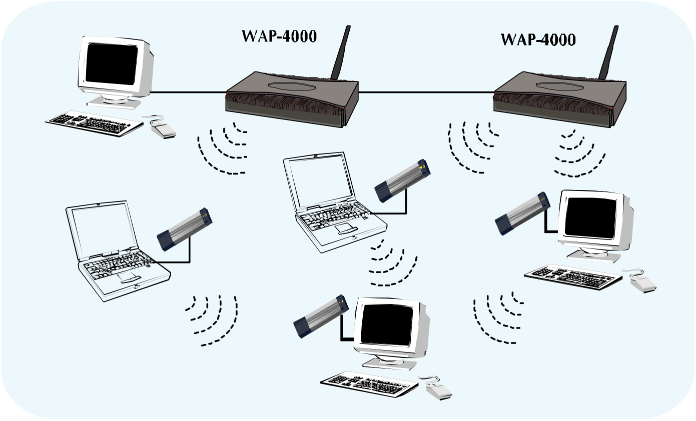
Infrastructure

The major difference between Infrastructure network and Ad-hoc wireless network is that the former requires an Access point. For old buildings, open areas, or frequently changing environments, just install the WL-U357 on your desktop or laptop, and thus you can get connected to the wired Ethernet through a wireless Access Point. SOHO users can then access the Internet and share all kinds of data with the other wired or wireless clients within the coverage of wireless signals. For enterprise users, the installation of multiple Access Points to enlarge the coverage of wireless signals can provide wireless users with seamless network access.

The Infrastructure mode is appropriate for enterprise-scale wireless access to a central database or provides various wireless applications for mobile users.

Infrastructure mode also supports roaming capabilities for mobile users. More than one BSS can be configured as an Extended Service Set (ESS). The continuous wireless network connectivity allows users to roam freely within an ESS. All wireless clients using WL-U357 or other IEEE 802.11b compliant wireless adapters within one ESS must be configured with the same ESS ID and to use the same radio channel.

Before adopting an ESS with roaming capability, choosing an available radio channel with less interference is highly recommended. Proper Access Point positioning combined with a clear radio channel will greatly enhance performance.

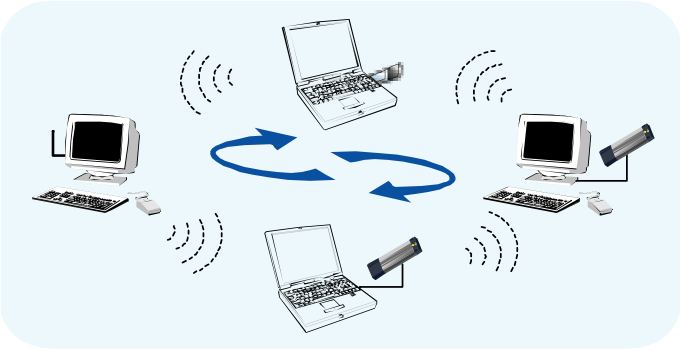


Ad-Hoc

Still complaining about the high price of wireless access points? This mode is the easiest and cost-effective way to meet your requirements. It enables you to construct wireless networking in no time without any access point.

Ad-hoc mode is a wireless network type in which a group of computers equipped with WL-U357 or other wireless adapters are connected together to form an independent wireless LAN. All computers operating in this mode must be configured to share the same radio channel.

In this scenario, new devices can be quickly added; however, wireless stations can only communicate with the other peers that belong to the same IBSS (Independent Basic Service Set).



General Application

WL-U357 offers a fast, reliable, cost-effective solution for wireless access to the various network scenarios:

1. Remote access to corporate network for information

E-mail, file transfer and terminal service.

2. Difficult-to-wire environments

Historical or old buildings, public occasions, venues and open area where it is difficult to wire.

3. Frequently changing environments

Factories, Retailers, and Offices that frequently change locations and rearrange the workplace

4. Temporary network access

Events, exhibitions, construction sites or some important occasions that require temporary network access.

5. Access to database for mobile workers

Doctors, nurses, retailers, white-collar workers who need access to database while roaming in the hospital, retail store or office.

6. SOHO (Small Office and Home Office) users

SOHO users who are in need of easy-to-install and wide coverage networking.

1.3 Specification

Attached Interface	USB 2.0 A-type connector
Operating Frequency / Channel	2.412~2.462GHz (FCC, Canada) / 11 Channels 2.412~2.472GHz (ETSI, Europe) / 13 Channels 2.412~2.484GHz (TELEC, Japan) / 14 Channels
Emission type	Direct Sequence Spread Spectrum (DSSS) Technology
RF Modulation	OFDM with BPSK, QPSK, 16QAM, 64QAM
RF Output Power	15dBm
Data Rate	802.11b: 1, 2, 5.5, 11Mbps 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps Super G: up to 108Mbps
Security	64/128/152bit WEP 802.1x WPA-PSK WPA-RADIUS
Antenna	Internal Patch Antenna
Sensitivity	IEEE802.11b: 2Mbps (QPSK): -87dBm 11 Mbps (QPSK): -82dBm (Typically @PER < 8% packet size 1024 and @25ºC + 5ºC) IEE802.11g: 54Mbps (64QAM): -66dBm 48Mbps (64QAM): -69dBm 36Mbps (16QAM): -74dBm 24Mbps (16QAM): -78dBm 18Mbps (QPSK): -82dBm 12Mbps (QPSK): -84dBm

	9Mbps (BPSK): -86dBm 6Mbps (BPSK): -88dBm (Typically @PER < 10% packet size 1024 and @25ºC + 5ºC)
Working Mode	Infrastructure, Ad-Hoc
Power Consumption	Continuous TX: 472mA, Continuous RX: 290mA
Compatibility	Windows 98SE/ME/2000/XP/Server 2003

1.4 Package Contents

Before installation, please check the items of your package. The package should include the following items:

- One Wireless USB Adapter
- One USB Cable
- One CD-ROM (Including the Configuration Utility, Driver and User's Manual)
- One Quick Installation Guide

If any of the above items is missing, contact your supplier as soon as possible.

1.5 Minimum System Requirements

Before installation, please check the following requirements with your equipment.

- Pentium Based (above) IBM-compatible PC system with one vacancy USB 1.1/2.0 port
- CD-ROM drive
- Windows 98SE/2000/ME/XP Operating System
- At least 5MBytes of free disk space for utility and driver installation

1.6 Installation Considerations

- Beware of the walls and ceilings. Each wall or ceiling can reduce your wireless cover range form 3-90 feet. Properly position your Access Points, Residential Gateways, and computers so that the number of walls or ceilings residing between Access Points and clients is minimized.
- Building materials make a difference – A solid metal door or aluminum studs may have a negative effect on signal coverage range. Try to properly position Access Points and computers with wireless adapters so that there would be less obstacles existing between them.
- Keep your wireless LAN devices away from microwaves, cordless phones and child incubators. It is likely that the latter will cause interferences to the operation of your wireless LAN devices.

Chapter 2 Installation Procedure

Before you proceed with the installation, it is necessary that you have enough information about the Wireless USB Adapter. Follow the procedure described below in this chapter to install the USB adapter under Windows 98SE/ME/2000/XP.

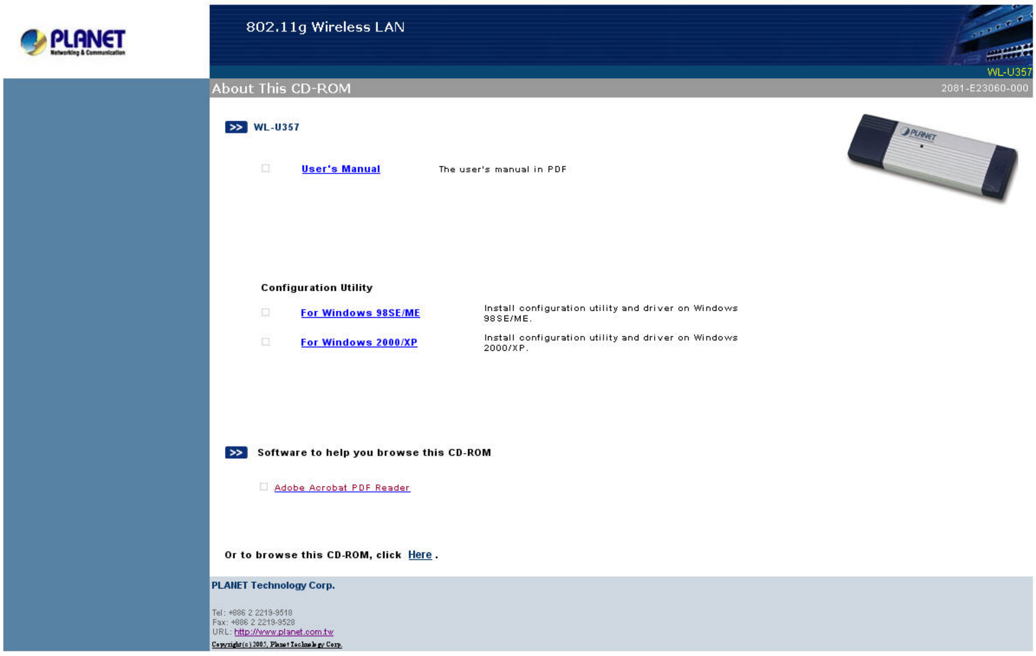
2.1 Configuration Utility & Driver Installation

The following installation operates under Window XP. The procedure also applies to Windows 98SE/ME/2000.

Note 1: If you had ever installed the other Wireless Cards before, please uninstall the existed drivers and utilities first.

Note 2: Please install the configuration utility before insert WL-U357 into the USB port of the computer.

A. Insert the bundled CD into the CD-ROM drive to launch the autorun program. Once completed, a menu screen will show up as follows.



802.11g Wireless LAN

WL-U357

About This CD-ROM

2081-E23060-000

>> WL-U357

□ User's Manual — The user's manual in PDF

Configuration Utility

□ For Windows 98SE/ME — Install configuration utility and driver on Windows 98SE/ME.

□ For Windows 2000/XP — Install configuration utility and driver on Windows 2000/XP.

>> Software to help you browse this CD-ROM

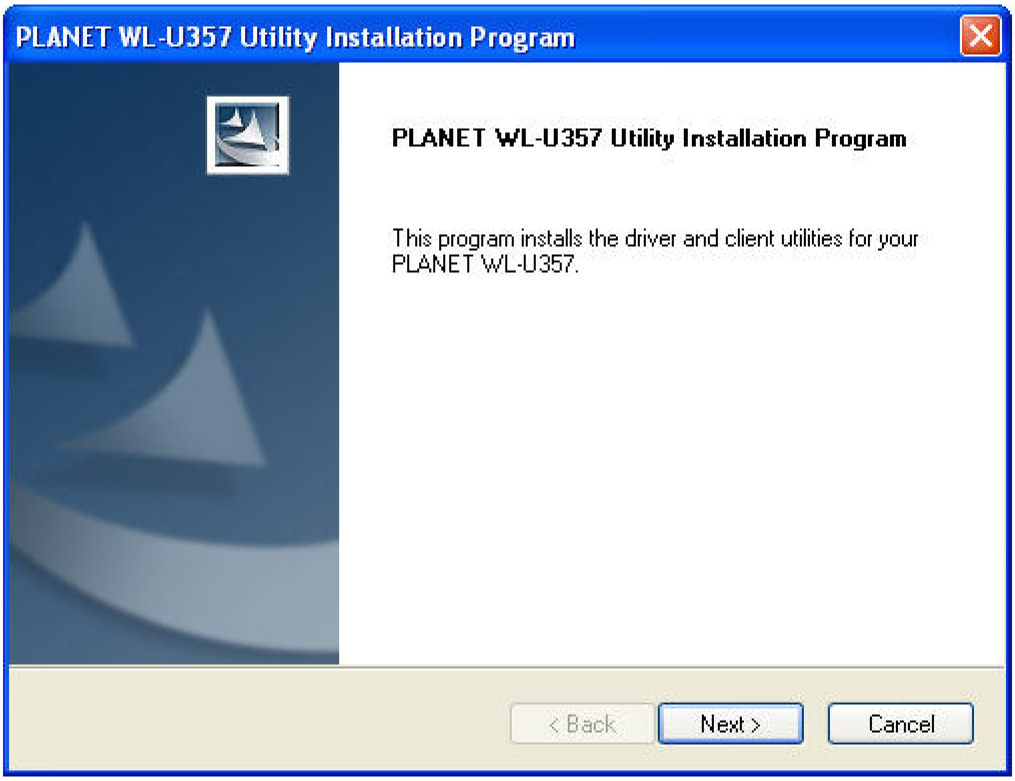
□ Adobe Acrobat PDF Reader

Or to browse this CD-ROM, click Here .

PLANET Technology Corp.

Tel: +886 2 2219-9518
Fax: +886 2 2219-9528
URL: http://www.planet.com.tw
Copyright(c) 2005, Planet Technology Corp.

B. Depending on the operating system you use, click on "For Windows 2000/XP" or "For Windows 98/ME" hyper link to initiate the installation procedure. You will see the below InstallShield Wizard window. Please click "Next" to continue.



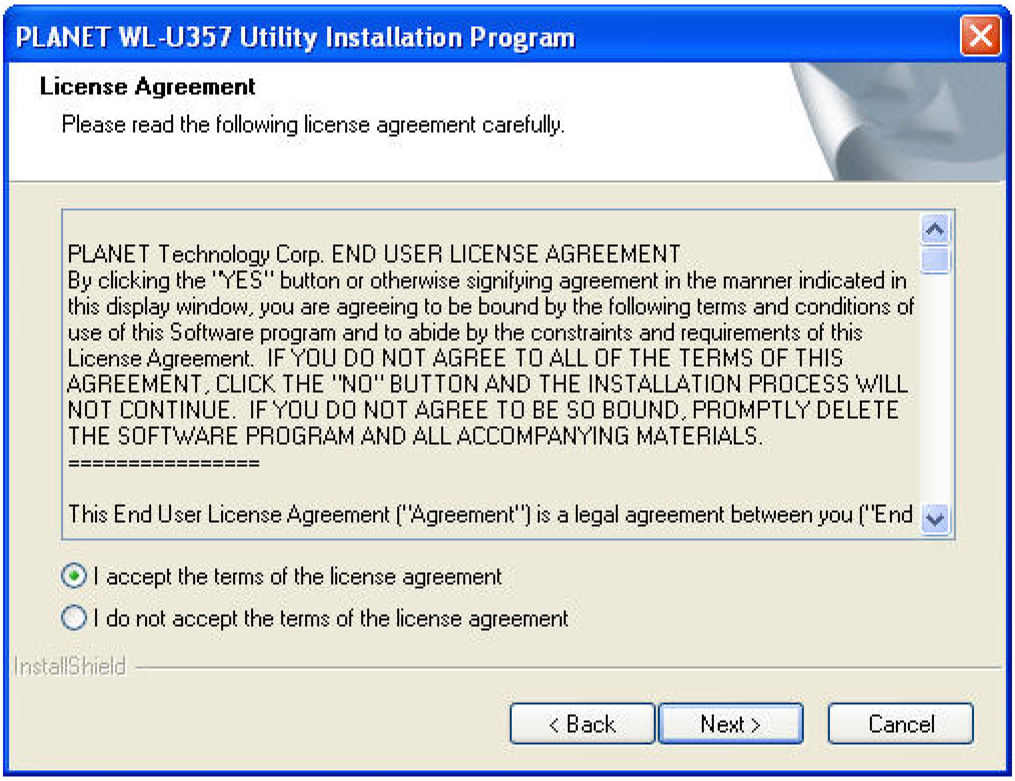
PLANET WL-U357 Utility Installation Program

PLANET WL-U357 Utility Installation Program

This program installs the driver and client utilities for your PLANET WL-U357.

Note: If the screen in step A does not appear, click "Start" at the taskbar. Then, select "Run" and type "E:\Utility" to access the folder, where E is your CD-ROM drive. Execute the appropriate utility for your operating system.

C. Select "I accept the terms of the license agreement" and click "Next" button to continue.



PLANET WL-U357 Utility Installation Program

License Agreement

Please read the following license agreement carefully.

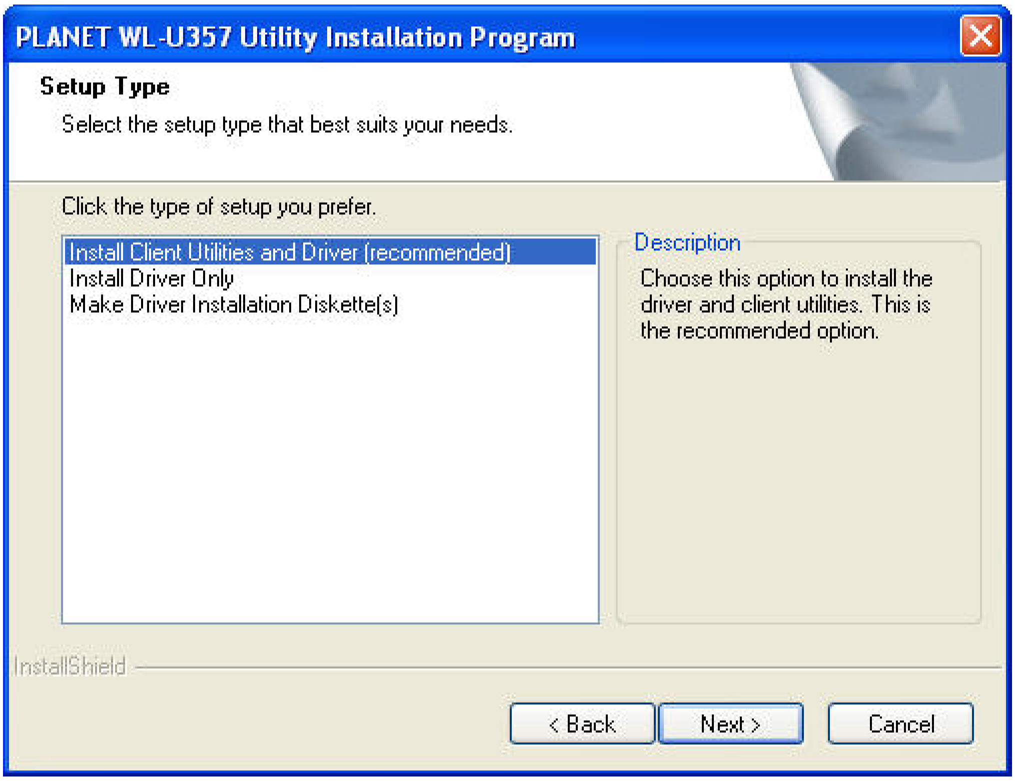
PLANET Technology Corp. END USER LICENSE AGREEMENT
By clicking the "YES" button or otherwise signifying agreement in the manner indicated in this display window, you are agreeing to be bound by the following terms and conditions of use of this Software program and to abide by the constraints and requirements of this License Agreement. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "NO" BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE. IF YOU DO NOT AGREE TO BE SO BOUND, PROMPTLY DELETE THE SOFTWARE PROGRAM AND ALL ACCOMPANYING MATERIALS.
================

This End User License Agreement ("Agreement") is a legal agreement between you ("End

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

D. Select "Install Client Utilities and Driver (recommended)" and click "Next" button to continue.


PLANET WL-U357 Utility Installation Program

Setup Type

Select the setup type that best suits your needs.

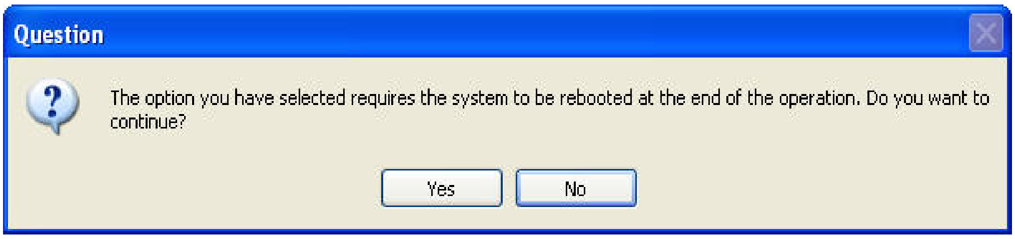
Click the type of setup you prefer.

- Install Client Utilities and Driver (recommended)
- Install Driver Only
- Make Driver Installation Diskette(s)

Description

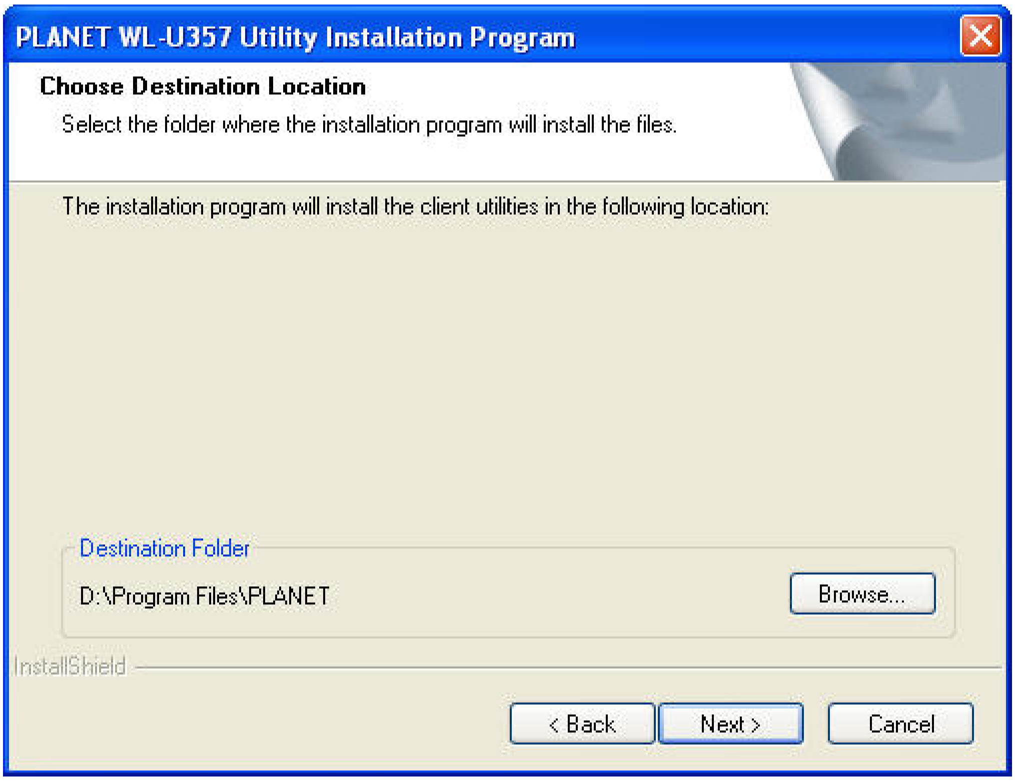
Choose this option to install the driver and client utilities. This is the recommended option.

E. Click "Yes" button to continue.


Question

The option you have selected requires the system to be rebooted at the end of the operation. Do you want to continue?

F. You can click "Browse" to specify the Destination Folder that you want to install the configuration utility. Or you can keep the default setting and click "Next" to continue.



PLANET WL-U357 Utility Installation Program

Choose Destination Location

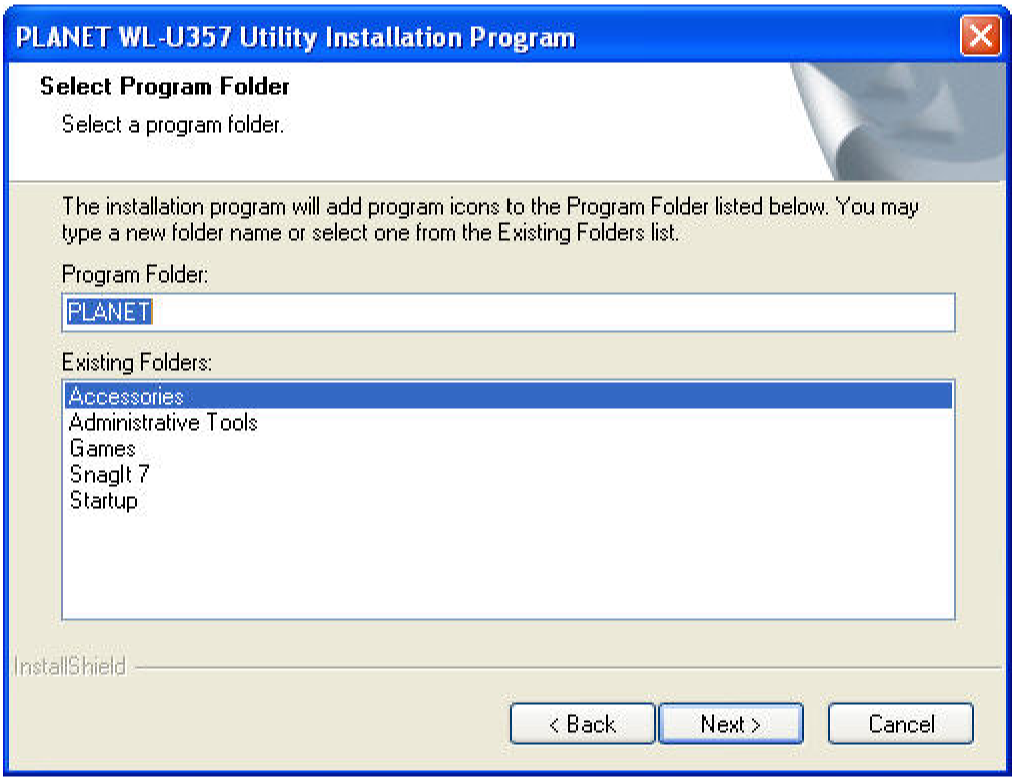
Select the folder where the installation program will install the files.

The installation program will install the client utilities in the following location:

Destination Folder

D:\Program Files\PLANET

G. Select the program folder you want to install this utility to. Or you can keep the default setting and click ”Next” to continue



PLANET WL-U357 Utility Installation Program

Select Program Folder

Select a program folder.

The installation program will add program icons to the Program Folder listed below. You may type a new folder name or select one from the Existing Folders list.

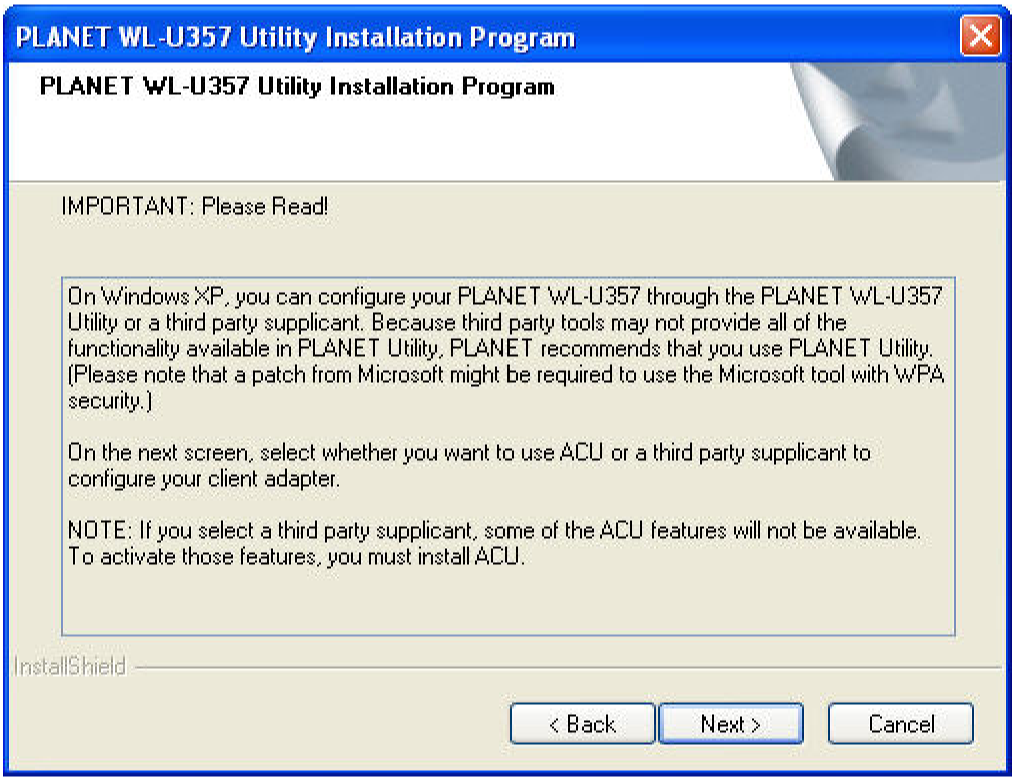
Program Folder:

PLANET

Existing Folders:

Accessories
Administrative Tools
Games
SnagIt 7
Startup

H. Click “Next” to continue



PLANET WL-U357 Utility Installation Program

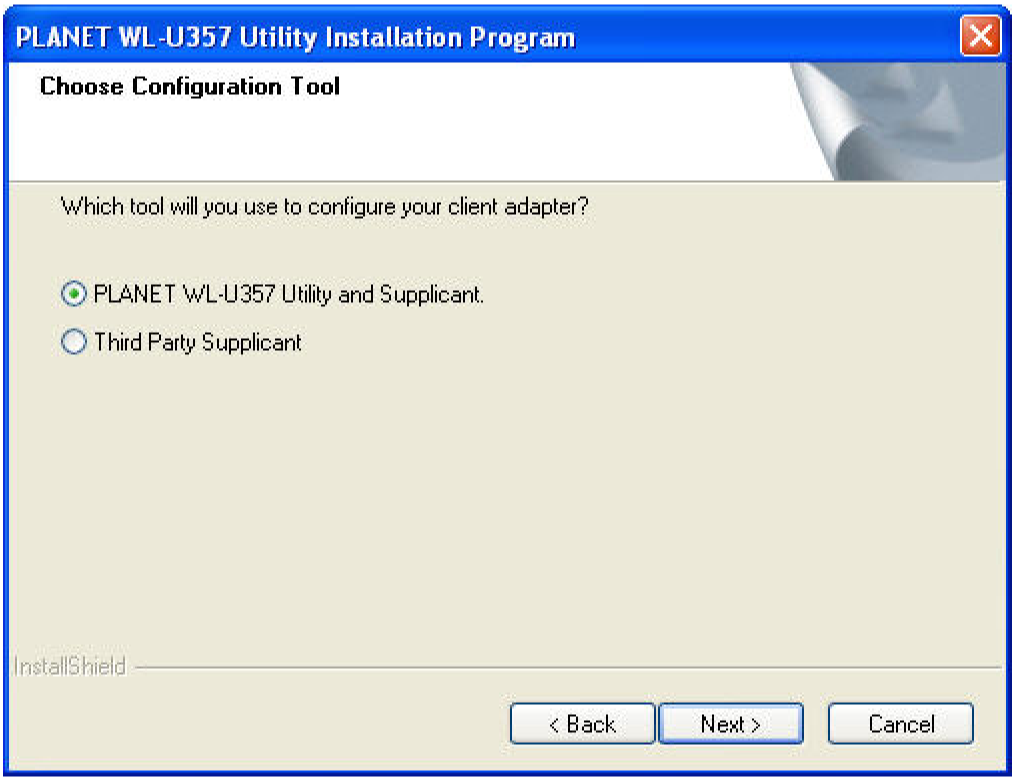
IMPORTANT: Please Read!

On Windows XP, you can configure your PLANET WL-U357 through the PLANET WL-U357 Utility or a third party supplicant. Because third party tools may not provide all of the functionality available in PLANET Utility, PLANET recommends that you use PLANET Utility. (Please note that a patch from Microsoft might be required to use the Microsoft tool with WPA security.)

On the next screen, select whether you want to use ACU or a third party supplicant to configure your client adapter.

NOTE: If you select a third party supplicant, some of the ACU features will not be available. To activate those features, you must install ACU.

I. It is recommended to select “PLANET WL-U357 Utility and Supplicant” option. If “Third Party Supplicant” is selected, some functions may not work normally. Click “Next” to continue



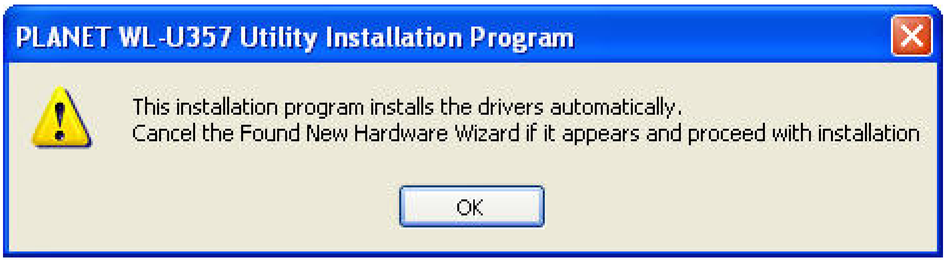
Choose Configuration Tool

Which tool will you use to configure your client adapter?

● PLANET WL-U357 Utility and Supplicant.

○ Third Party Supplicant

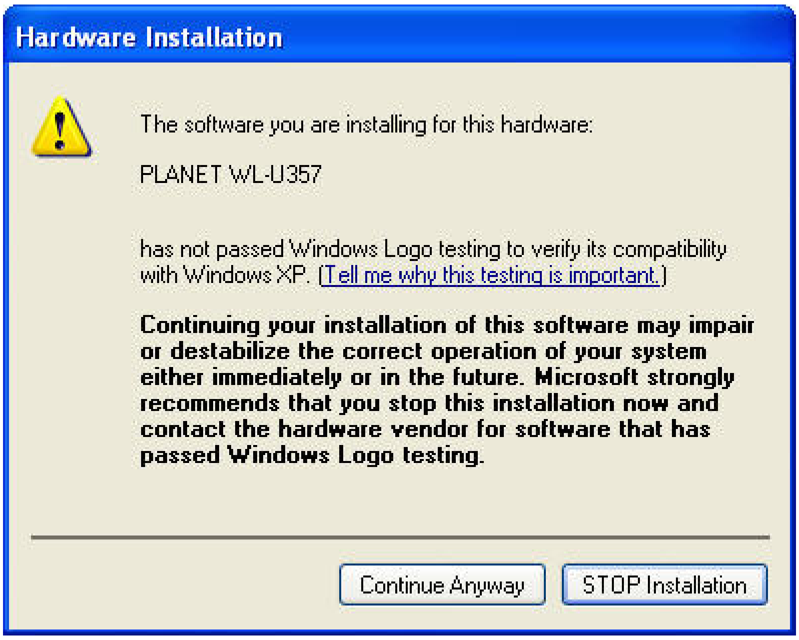
J. Insert WL-U357 when the dialog box pops up. Click “OK” to continue.



PLANET WL-U357 Utility Installation Program

This installation program installs the drivers automatically.
Cancel the Found New Hardware Wizard if it appears and proceed with installation

K. Click “Continue Anyway” to continue



Hardware Installation

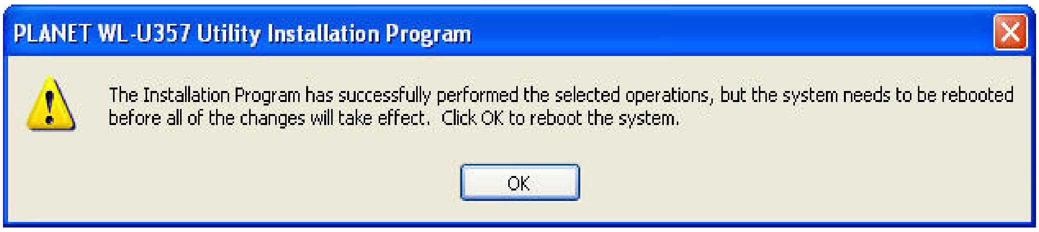
The software you are installing for this hardware:

PLANET WL-U357

has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.

L. Select “OK” to restart your computer right away



PLANET WL-U357 Utility Installation Program

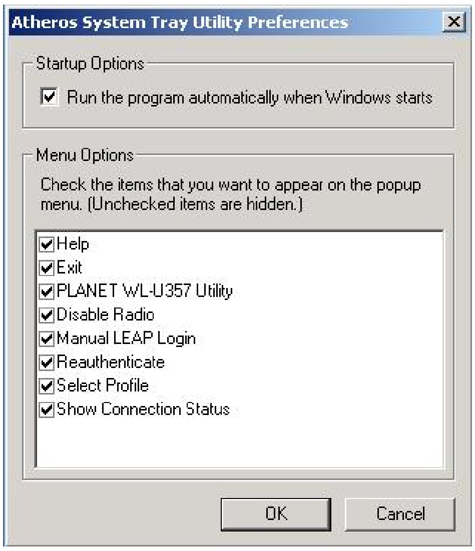
The Installation Program has successfully performed the selected operations, but the system needs to be rebooted before all of the changes will take effect. Click OK to reboot the system.

Chapter 3 Configuration Utility

The Configuration Utility is a powerful tool that helps you to configure WL-U357 easily and monitor the status of wireless communication.

Right-click the icon in the system tray, there are some items for you to use the configuration utility:

- Help: Show Manual Webpage.
- Exit: Select this to close the configuration utility tool.
- Open PLANET WL-U357 Utility: It enables you to open the configuration utility tool.
- Preferences: Select what you want to appear on the popup menu.



Atheros System Tray Utility Preferences

Startup Options

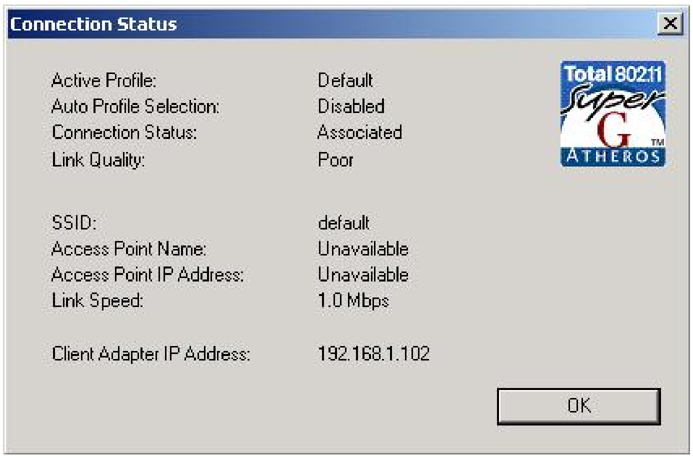
☑ Run the program automatically when Windows starts

Menu Options

Check the items that you want to appear on the popup menu. (Unchecked items are hidden.)

☑ Help
☑ Exit
☑ PLANET WL-U357 Utility
☑ Disable Radio
☑ Manual LEAP Login
☑ Reauthenticate
☑ Select Profile
☑ Show Connection Status

- Disable Radio: Disable RF signals
- Select Profile: Select profile that you want to use
- Show Connection Status: Show Connection Status such as Active Profile etc.



Connection Status

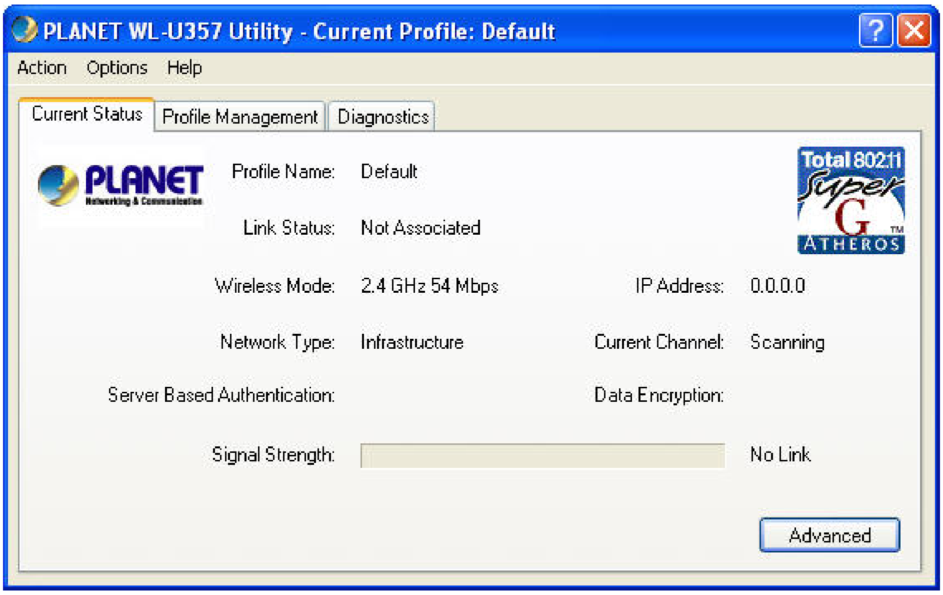
Active Profile: Default
Auto Profile Selection: Disabled
Connection Status: Associated
Link Quality: Poor

SSID: default
Access Point Name: Unavailable
Access Point IP Address: Unavailable
Link Speed: 1.0 Mbps

Client Adapter IP Address: 192.168.1.102

3.1 Current Status

When you open the configuration utility, the system will scan all the channels to locate available access points and wireless stations within the signal coverage. Then it will automatically connect to the access point or wireless station with the strongest signal strength. This screen displays all the information about the current wireless connection.


PLANET WL-U357 Utility - Current Profile: Default
Action
Options
Help
Current Status
Profile Management
Diagnostics
PLANET Networking & Communication
Total 802.11 Super G ATHEROS
Advanced

Profile Name: Default

Link Status: Not Associated

Wireless Mode: 2.4 GHz 54 Mbps

IP Address: 0.0.0.0

Network Type: Infrastructure

Current Channel: Scanning

Server Based Authentication:

Data Encryption:

Signal Strength: No Link

Profile Name	The name of the current selected configuration profile.
Link Status	Shows whether the station is associated to the wireless network.
Wireless Mode	Displays the wireless mode.
IP Address	Displays the computer's IP address.
Network Type	The type of network the station is connected to. The options include Infrastructure (access point) and Ad Hoc.
Current Channel	Shows the currently connected channel.
Server Based Authentication	Shows whether server based authentication is used.
Data Encryption	Displays the encryption type the adapter is using.
Signal Strength	Shows the strength of the signal.

Click the Advanced button to see the advanced status diagnostics.

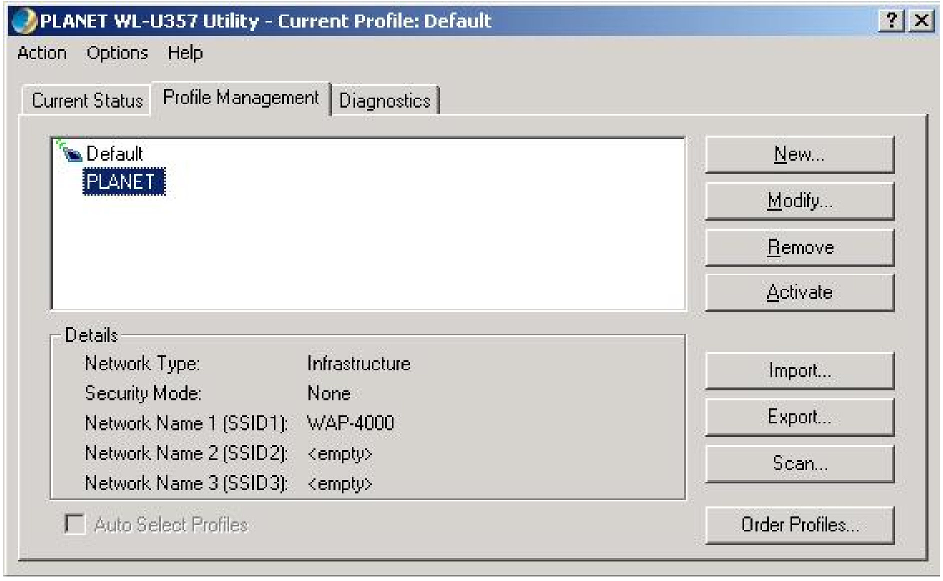
Network Name (SSID)	Displays the wireless network name.
Server Based Authentication	Shows whether server based authentication is used.
Data Encryption	Displays the encryption type the adapter is using.

Authentication Type	Displays the authentication mode. .
Message Integrity Check	Shows whether MIC is enabled. MIC prevents bit-flip attacks on encrypted packets.
Associated AP Name	Displays the name of the access point the wireless adapter is associated to.
Associated AP IP Address	Shows the IP address of the access point the wireless adapter is associated to.
Associated AP MAC Address	Displays the MAC address of the access point the wireless adapter is associated to.
Power Save Mode	Shows the power save mode. Power management is disabled in ad hoc mode.
Current Power Level	Displays the transmit power level rate in mW.
Available Power Levels	Shows the 802.11b/g available power levels.
Current Signal Strength	Shows the current signal strength in dBm.
Current Noise Level	Displays the current noise level in dBm.
Up Time	Shows how long the client adapter has been receiving power (in hours:minutes:seconds). If the adapter runs for more than 24 hours, the display shows in days:hours:minutes:seconds.
802.11b Preamble	Displays the 802.11b preamble format.
Current Receive Rate	Shows the current receive rate in Mbps.
Current Transmit Rate	Displays the current transmit rate in Mbps.
Channel	Shows the currently connected channel.
Frequency	Displays frequency the station is using.
Channel Set	Shows the current channel set.

Menu Bar

- **Action:**
  - Disable Radio: Disable RF signals.
  - Disable Tray Icon: Disable the utility icon 📶 in the system tray.
  - Exit: Select this to close the configuration utility tool.
- **Options:** Select the display units of the Signal strength or Data.
- **Help:**
  - PLANET WL-U357 Utility Help: display Manual Webpage.
  - About PLANET WL-U357 Utility: display Utility Version.

3.2 Profile Management



Default
PLANET

Details

Network Type: Infrastructure
Security Mode: None
Network Name 1 (SSID1): WAP-4000
Network Name 2 (SSID2): <empty>
Network Name 3 (SSID3): <empty>

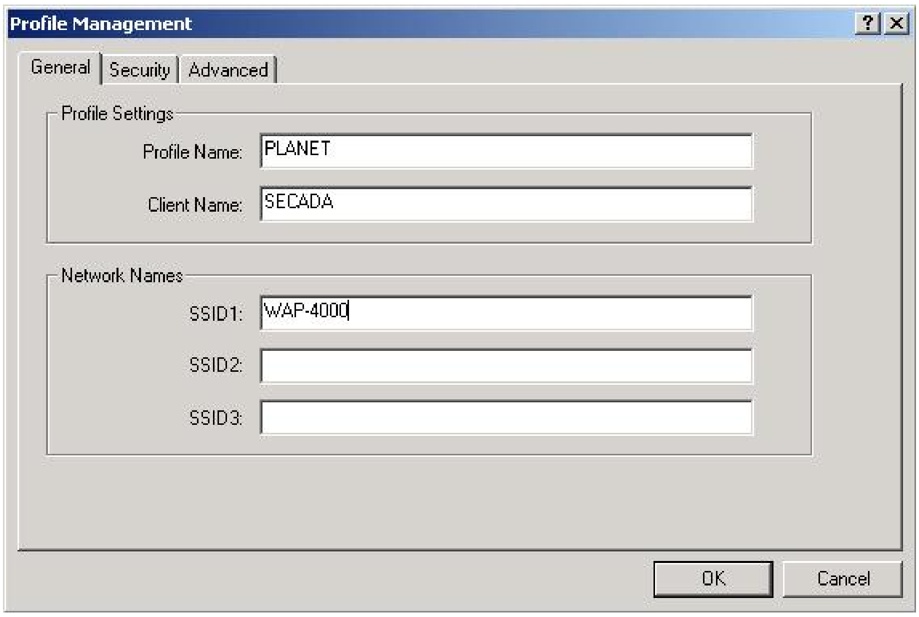
□ Auto Select Profiles

3.2.1 Add a Profile

To add a new configuration profile, click New on the Profile Management tab. The Profile Management dialog box displays the General tab.

Please note that the WL-U357 utility only allows the creation of 16 configuration profiles. After the creation of 16 profiles, clicking the New button displays an error message

3.2.1.1 General Tab



Profile Settings

Profile Name: PLANET

Client Name: SECADA

Network Names

SSID1: WAP-4000

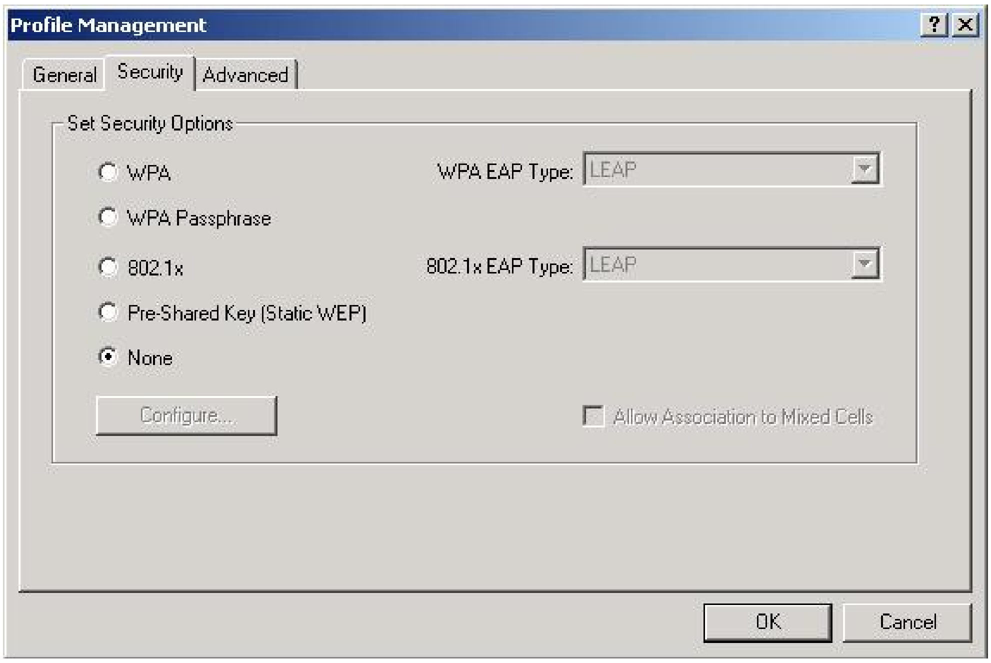
SSID2:

SSID3:

Profile Name	Identifies the configuration profile. This name must be unique. Profile names are not case sensitive.
Client Name	Identifies the client machine.

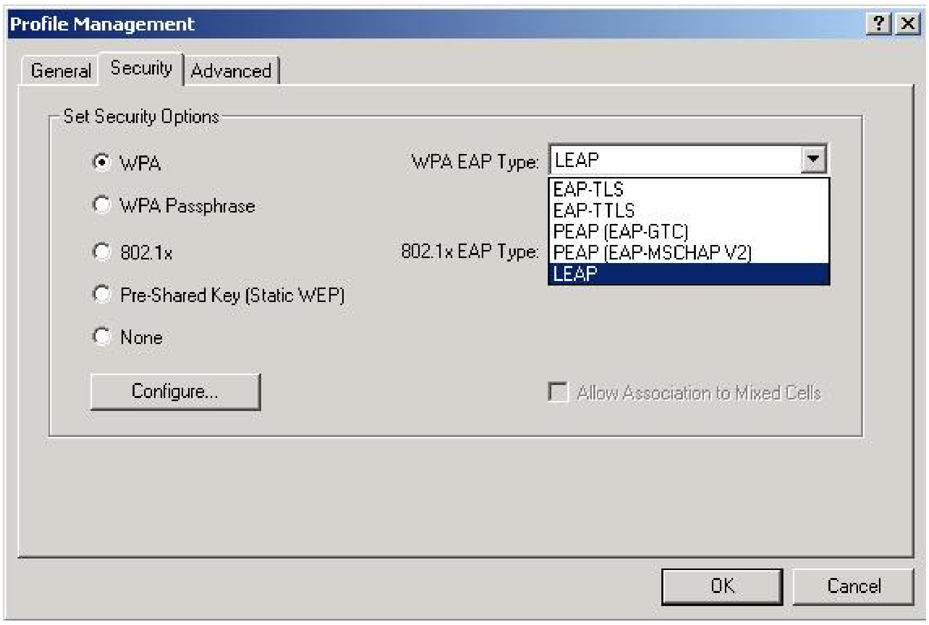
Network Names (SSIDs)	The IEEE 802.11 wireless network name. This field has a maximum limit of 32 characters. WL-U357 can configure up to three SSIDs (SSID1, SSID2, and SSID3).

3.2.1.2 Security Tab



This section describes the security settings of the PLANET WL-U357 Utility.

WPA & 802.1x Setting



Using EAP-TLS Security

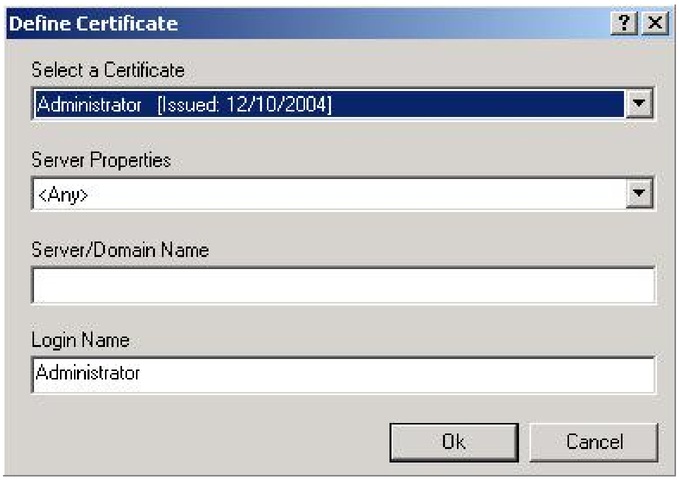
To use EAP-TLS security, the machine must already have the EAP-TLS certificates downloaded onto it. Check with the IT manager.

1. On the Security tab, choose the WPA radio button.

   OR: On the Security tab, choose the 802.1x radio button.

2. Choose EAP-TLS from the drop-down menu.

3. Click the Configure button.



Define Certificate

Select a Certificate: Administrator [Issued: 12/10/2004]

Server Properties: <Any>

Server/Domain Name:

Login Name: Administrator

4. Select the appropriate certificate authority from the list. The server/domain name and the login name are filled in automatically from the certificate information. Click OK.

5. Activate the profile.

Using EAP-TTLS Security

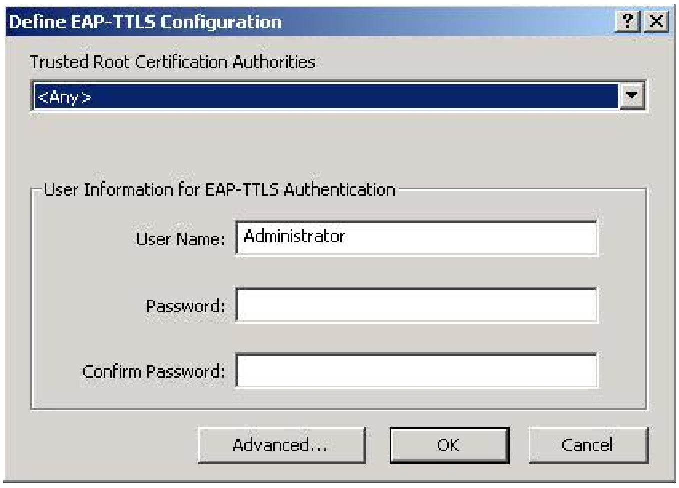
To use EAP-TTLS security, the machine must already have the EAP-TTLS certificates downloaded onto it. Check with the IT manager.

1. On the Security tab, choose the WPA radio button.

   OR: On the Security tab, choose the 802.1x radio button.

2. Choose EAP-TTLS from the drop-down menu.

3. Click the Configure button.



Define EAP-TTLS Configuration

Trusted Root Certification Authorities

<Any>

User Information for EAP-TTLS Authentication

User Name: Administrator

Password:

Confirm Password:

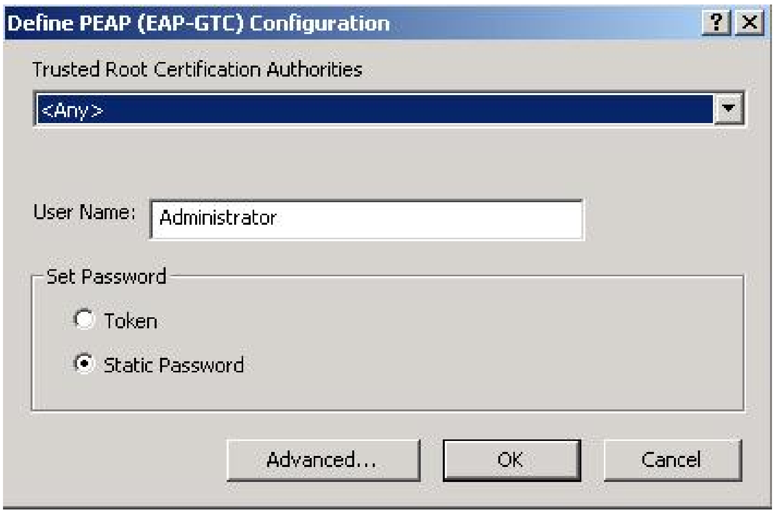
4. Select the appropriate certificate from the drop-down list and click OK.
5. Enter a EAP user name in the User Name field and password and start the EAP authentication process.
6. Click Advanced and:
   - Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. **(recommended)**
   - Enter the domain name of the server from which the client will accept a certificate.
   - Change the login name if needed.
7. Click OK.
8. Enable the profile.

Using PEAP-GTC Security

To use PEAP (EAP-GTC) security, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager.

1. On the Security tab, choose the WPA radio button.
   OR: On the Security tab, choose the 802.1x radio button.
2. Choose PEAP (EAP-GTC) from the drop-down menu.

3. Click the Configure button.



Define PEAP (EAP-GTC) Configuration

Trusted Root Certification Authorities

<Any>

User Name: Administrator

Set Password

○ Token

● Static Password

4. Select the appropriate network certificate authority from the drop-down list.

5. Enter a PEAP user name in the User Name field to use a separate user name and start the PEAP authentication process.

6. Choose Token or Static Password, depending on the user database.
   Note that Token uses a hardware token device or the Secure Computing SofToken program (version 1.3 or later) to obtain and enter a one-time password during authentication.

7. Click Advanced and:

   - Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. **(recommended)**

   - Enter the domain name of the server from which the client will accept a certificate.

   - The login name used for PEAP tunnel authentication, fills in automatically as PEAP-xxxxxxxxxxxx, where xxxxxxxxxxxx is the computer's MAC address.   Change the login name if needed.

8. Click OK.

9. Enable the profile.

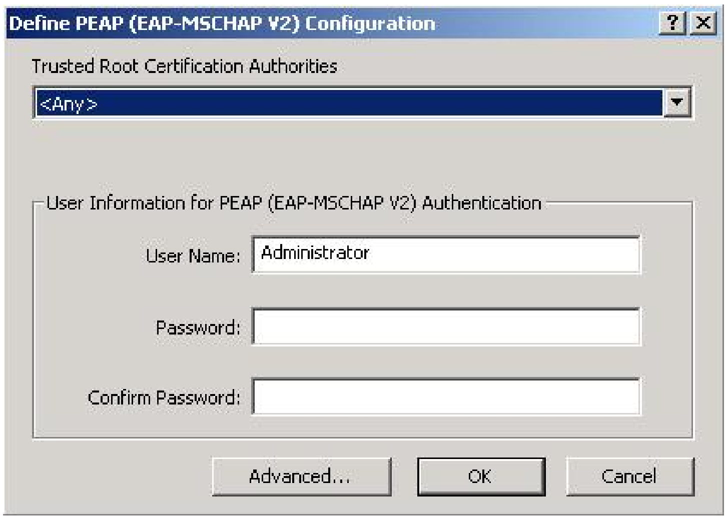
Using PEAP-MSCHAP V2 Security

To use PEAP (EAP-MSCHAP V2) security, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager.

1. On the Security tab, choose the WPA radio button.
   OR: On the Security tab, choose the 802.1x radio button.

2. Choose PEAP (EAP-MSCHAP V2) from the drop-down menu.

3. Click the Configure button.



Define PEAP (EAP-MSCHAP V2) Configuration

Trusted Root Certification Authorities

<Any>

User Information for PEAP (EAP-MSCHAP V2) Authentication

User Name: Administrator

Password:

Confirm Password:

4. Select the appropriate certificate from the drop-down list.

5. Enter a PEAP user name in the User Name field to use a separate user name and start the PEAP authentication process.

6. Click Advanced and:

   - Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. **(recommended)**
   - Enter the domain name of the server from which the client will accept a certificate.
   - The login name used for PEAP tunnel authentication, fills in automatically as PEAP-*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the computer's MAC address. Change the login name if needed.

7. Click OK.

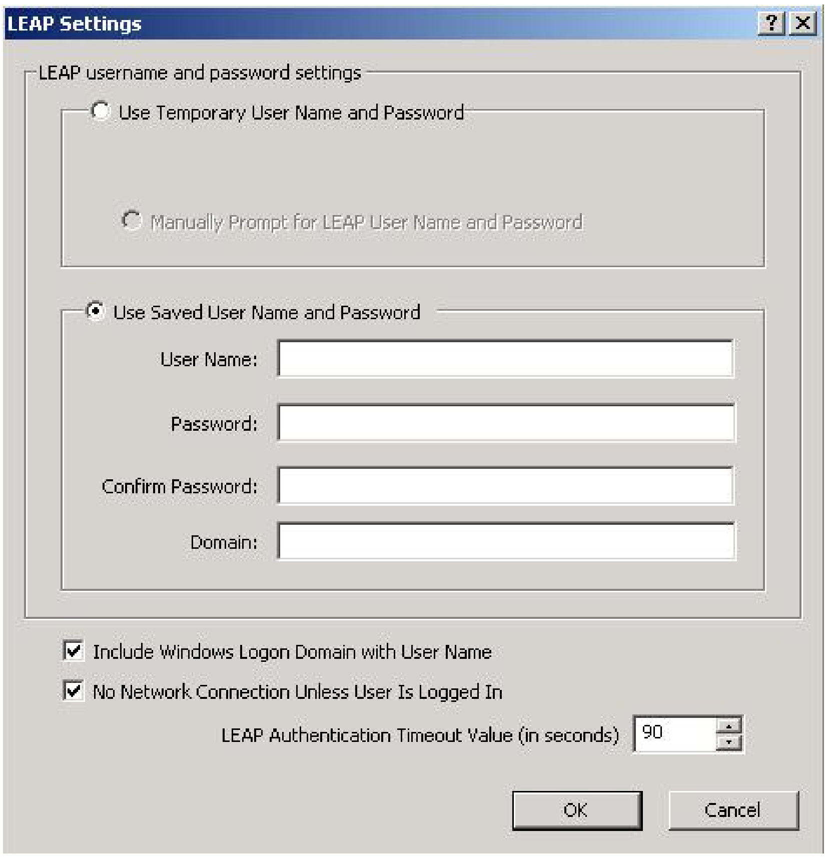
8. Enable the profile.

Using LEAP Security

LEAP security requires that all infrastructure devices (e.g. access points and servers) are configured for LEAP authentication. Check with the IT manager.

1. On the Security tab, choose the WPA radio button. Choose WPA-LEAP from the drop-down menu.
   OR: On the Security tab, choose the 802.1x radio button. Choose LEAP from the drop-down menu.

2. Click the Configure button.



LEAP Settings

LEAP username and password settings

○ Use Temporary User Name and Password

○ Manually Prompt for LEAP User Name and Password

● Use Saved User Name and Password

User Name:

Password:

Confirm Password:

Domain:

☑ Include Windows Logon Domain with User Name

☑ No Network Connection Unless User Is Logged In

LEAP Authentication Timeout Value (in seconds) 90

3. Select to Use Temporary User Name and Password by choosing the radio button. Check Manually Prompt for LEAP User Name and Password to manually login and start the LEAP authentication process.

4. Select to Use Saved User Name and Password by choosing the radio button and specify the LEAP user name, password, and domain to save and use.

5. Specify a domain name:

   ○ Check the Include Windows Logon Domain with User Name setting to pass the Windows login domain and user name to the RADIUS server. **(default)**

   ○ OR: Enter a specific domain name.

6. If desired, check No Network Connection Unless User Is Logged In to force the wireless adapter to disassociate after logging off.

7. Enter the LEAP authentication timeout time (between 30 and 500 seconds) to specify how long LEAP should wait before declaring authentication failed, and sending an error message. The default is 90 seconds.

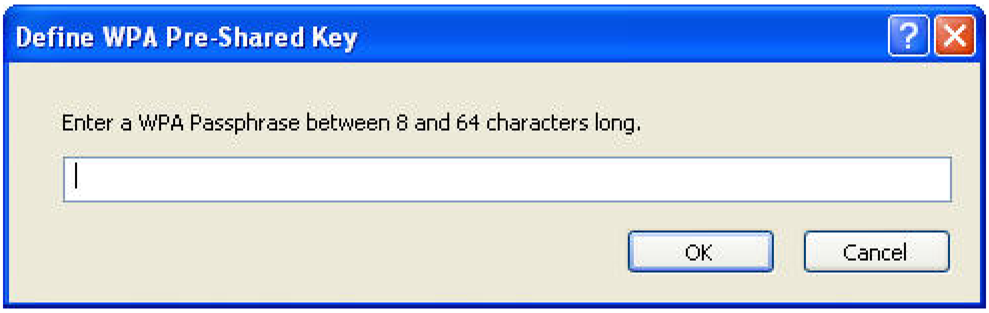
8. Click OK.

9. Enable the profile.

WPA Passphrase Setting

1. On the Security tab, choose the WPA Passphrase radio button

2. Click on the Configure button.



Define WPA Pre-Shared Key

Enter a WPA Passphrase between 8 and 64 characters long.

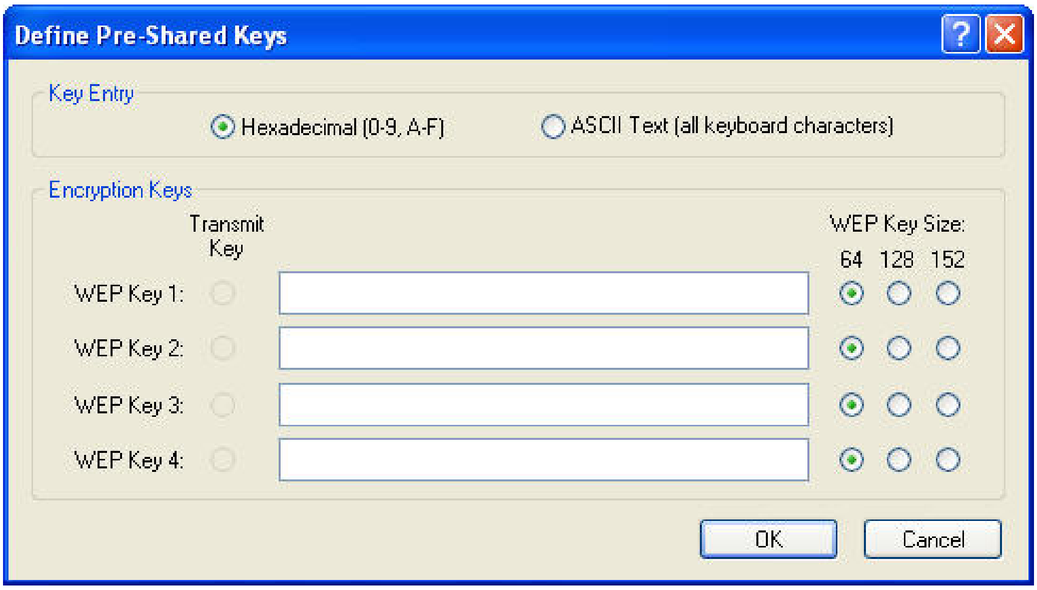
3. Fill in the WPA Passphrase

4. Click OK

Pre-Shared Key setting

1. Click the Define Pre-Shared Keys radio button on the Security tab.

2. Click on Configure button.



Define Pre-Shared Keys

Key Entry

● Hexadecimal (0-9, A-F) ○ ASCII Text (all keyboard characters)

Encryption Keys

	Transmit Key		64	128	152
WEP Key 1:	○		●	○	○
WEP Key 2:	○		●	○	○
WEP Key 3:	○		●	○	○
WEP Key 4:	○		●	○	○

3. Fill in the fields in the Define Pre-Shared Keys dialog box

4. Click OK for the changes to take effect

Key Button	Description
Key Entry	Determines the entry method for an encryption key: hexadecimal (0-9, A-F), or ASCII text (all keyboard characters except spaces).
Encryption Keys	Selects the default encryption keys used. Only allows the selection for a shared First, Second, Third, or Fourth key whose corresponding field has been completed.
WEP Keys (1-4)	Defines a set of shared encryption keys for network configuration security. At least one Shared Key field must be populated to enable security using a shared key. Click on the radio button to set the key as the default encryption key.
WEP Key Size	Defines the size for each encryption key. The options include: ○ 64- bit (enter 10 digits for hexadecimal, 5 ASCII characters) ○ 128- bit (enter 26 digits for hexadecimal, 13 digits for ASCII) ○ 152-bit (enter 32 digits hexadecimal, 16 digits for ASCII)

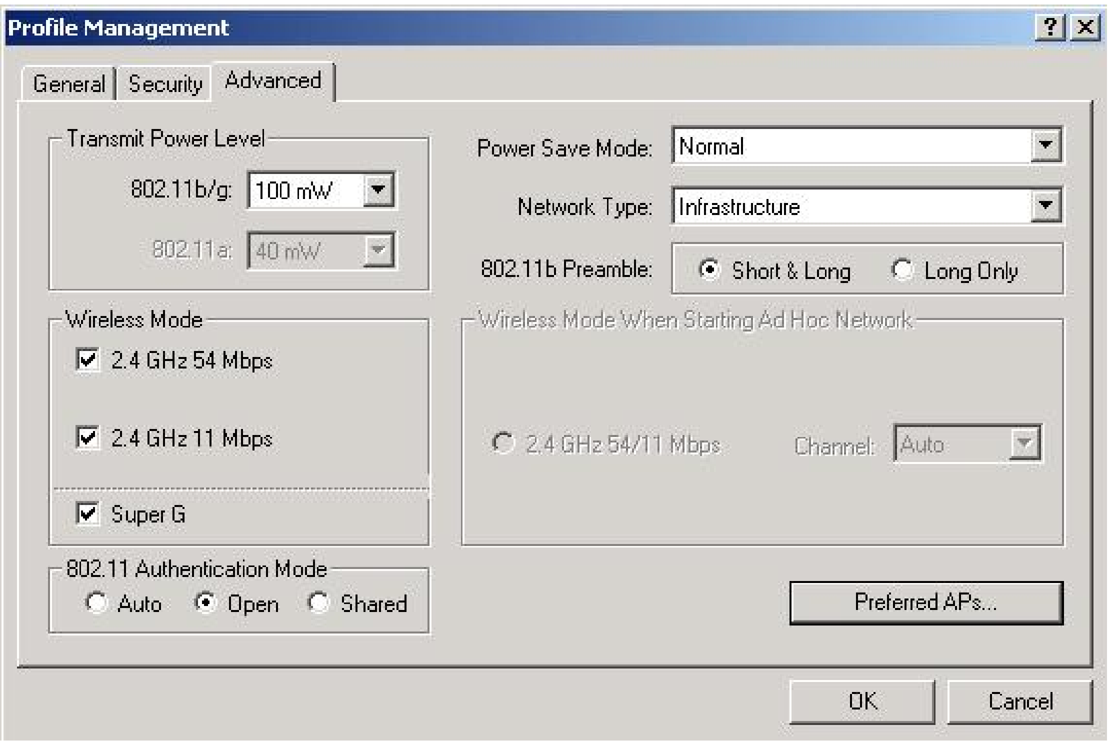
Overwriting an Existing Static WEP Key

1. Click the Pre-Shared Key radio button on the Security tab.
2. Click on Configure.
3. In the window, all existing static WEP keys are displayed as asterisks for security reasons. Click in the field of the existing static WEP key to overwrite.
4. Delete the asterisks in that field.
5. Enter a new key.
6. Make sure to select the Transmit Key button to the left of this key is selected for the key to transmit packets.
7. Click OK.

Disabling Static WEP

- To disable static WEP for a particular profile, choose None on the Profile Management tab and click OK.
- OR: Select any other security option on the Profile Management tab to automatically disable static WEP.

3.2.1.3 Advanced Tab



Profile Management

General | Security | Advanced

Transmit Power Level

802.11b/g: 100 mW

802.11a: 40 mW

Power Save Mode: Normal

Network Type: Infrastructure

802.11b Preamble: ● Short & Long ○ Long Only

Wireless Mode

☑ 2.4 GHz 54 Mbps

☑ 2.4 GHz 11 Mbps

☑ Super G

Wireless Mode When Starting Ad Hoc Network

○ 2.4 GHz 54/11 Mbps Channel: Auto

802.11 Authentication Mode

○ Auto ● Open ○ Shared

Transmit Power Level	Selects the transmit power level for 80211b/g in mW. Actual transmit power may be limited by regulatory domain or hardware limitations.
Power Save Mode	• **Maximum**: causes the access point to buffer incoming messages for the wireless adapter. The adapter up periodically polls the access point to see if any messages are waiting. • **Normal**: uses maximum when retrieving a large number of packets, then switches back to power save mode after retrieving the packets. • **Off**: turns power saving off, thus powering up the wireless adapter continuously for a short message response time.
Network Type	Specifies the network as either infrastructure (access point mode) or ad hoc.
802.11b Preamble	Specifies the preamble setting in 802.11b. The default setting is **Short & Long** (access point mode), which allows both short and long headers in the 802.11b frames. The adapter can only use short radio headers if the access point supports and uses them. Set to **Long Only** to override allowing short frames.
Wireless Mode	Specifies 2.4 GHz 54 Mbps, 2.4 GHz 11 Mbps, or Super G operation in an

	access point network. The wireless adapter must match the wireless mode of the access point it associates to.
Wireless Mode when Starting an Ad Hoc Network	This mode allows selection of the channel the wireless adapter uses. The channels available depend on the regulatory domain. If the adapter finds no other ad hoc adapters, this selection specifies which channel with the adapter starts the ad hoc network with. The wireless adapter must match the wireless mode and channel of the clients it associates to.
802.11a Authentication Mode	Select what mode the wireless adapter uses to authenticate to an access point: • **Auto:** causes the adapter to attempt authentication using shared, but switches it to open authentication if shared fails. • **Open:** enables an adapter to attempt authentication regardless of its WEP settings. It will only associate with the access point if the WEP keys on both the adapter and the access point match. • **Shared:** only allows the adapter to associate with access points that have the same WEP key.

For infrastructure (access point) networks, click the Preferred APs button to specify up to four access points to which the client adapter should attempt to associate.

3.2.2 Modify a Profile

To modify a configuration profile, select the configuration from the Profile list and click the Modify button. Please refer to above sections for detailed explanations about the settings.

3.2.3 Remove a Profile

To remove a configuration profile, select the configuration from the Profile list and click the Remove button.

The WL-U357 utility only allows the creation of 16 configuration profiles. After the creation of 16 profiles, clicking the New button displays an error message. Remove an old profile or modify an existing profile for a new use.

3.2.4 Switch Profiles

1. To switch to a different profile, go to the Profile Management tab.
2. Click on the profile name in the Profile List.
3. Click the Activate button.

3.2.5 Import a Profile

1. From the Profile Management tab, click the Import button. The Import Profile window appears.
2. Browse to the directory where the profile is located.
3. Highlight the profile name.
4. Click Open. The imported profile appears in the profiles list.

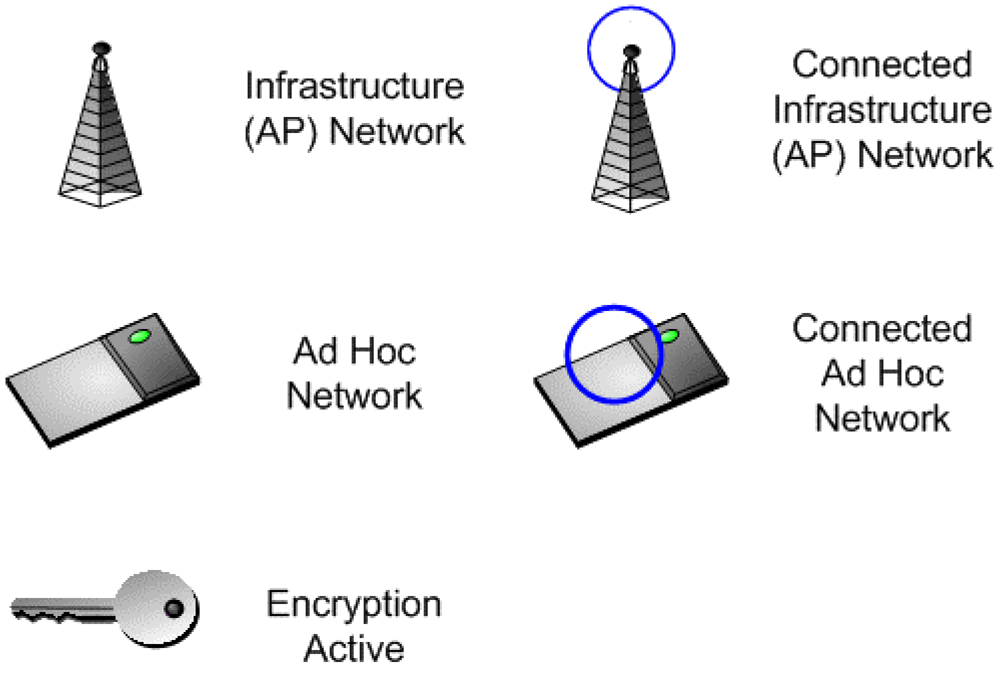
3.2.6 Export a Profile

1. From the Profile Management tab, highlight the profile to export.
2. Click the Export button. The Export Profile window appears.
3. Browse to the directory to export the profile to.
4. Click Save. The profile is exported to the specified location

3.2.7 Scan for Available Networks

Click the Scan button on the Profile Management tab to scan for available infrastructure and ad hoc networks. On this list, click Refresh to refresh the list at any time.

The Scan Result List provides icons below that specify the operational state and the signal strength for available stations.


Infrastructure (AP) Network
Connected Infrastructure (AP) Network
Ad Hoc Network
Connected Ad Hoc Network
Encryption Active

3.2.8 Auto Profile Selection Management

Including a profile in the auto selection feature allows the wireless adapter to automatically select that profile from the list of profiles and use it to connect to the network.

Including a profile in auto profile selection:

1. On the Profile Management tab, click the Order Profiles button.
2. The Auto Profile Selection Management window appears, with a list of all created profiles in the Available Profiles box.
3. Highlight the profiles to add to auto profile selection, then click Add. The profiles appear in the Auto Selected Profiles box.

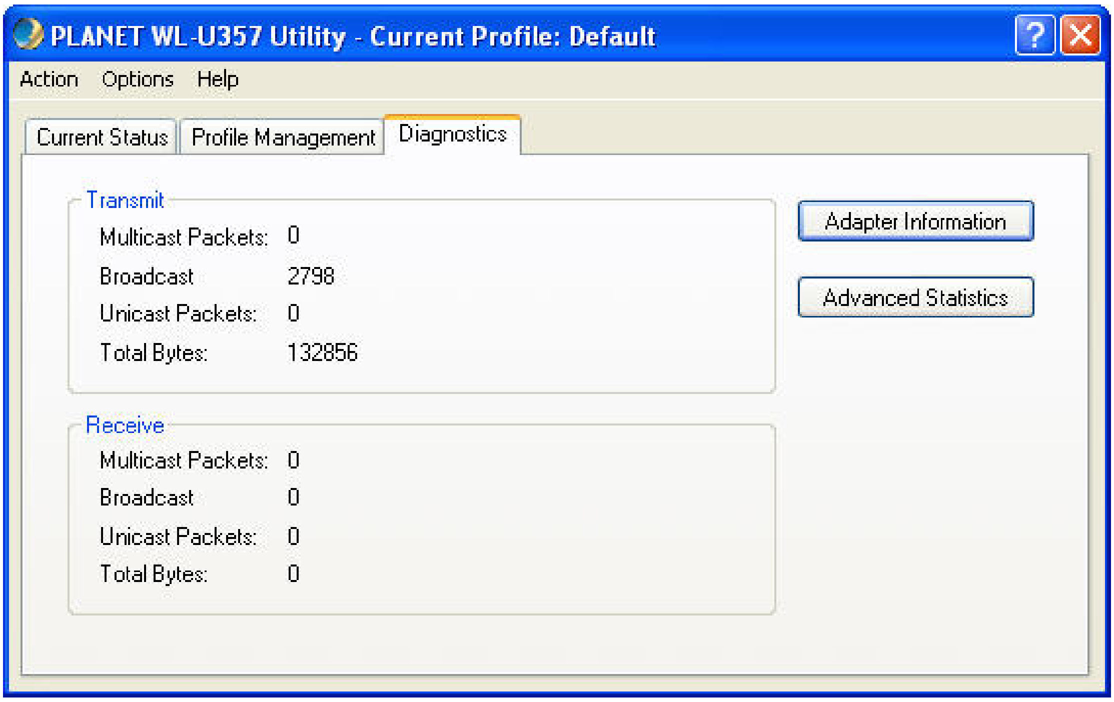
Ordering the auto selected profiles:

1. Highlight a profile in the Auto Selected Profiles box.
2. Click Move Up or Move Down as appropriate.

   The first profile in the Auto Selected Profiles box has highest priority, and the last profile has lowest priority.
3. Click OK.
4. Check the Auto Select Profiles box.
5. Save the modified configuration file.

When auto profile selection is enabled by checking Auto Select Profiles on the Profile Management tab, the client adapter scans for an available network. The profile with the highest priority and the same SSID as one of the found networks is the one that is used to connect to the network. If the connection fails, the client adapter tries the next highest priority profile that matches the SSID, and so on.

3.3 Diagnostics



Transmit

Multicast Packets: 0

Broadcast 2798

Unicast Packets: 0

Total Bytes: 132856

Receive

Multicast Packets: 0

Broadcast 0

Unicast Packets: 0

Total Bytes: 0

The Diagnostics tab of the WL-U357 Utility provides buttons used to retrieve receive and transmit statistics. The Diagnostics tab does not require any configuration.

The Diagnostics tab lists the following receive and transmit diagnostics for frames received by or transmitted by the wireless network adapter:

- Multicast frames transmitted and received
- Broadcast frames transmitted and received
- Unicast frames transmitted and received
- Total bytes transmitted and received

Click the Adapter Information button for more general information about the WL-U357 and its driver.

Click the Advanced Statistics button on the Diagnostics tab to also show receive and transmit statistical information for the following receive and transmit diagnostics for frames received by or transmitted to the WL-U357:

Transmitted Frames

- Frames transmitted OK
- Frames retried
- Frames dropped
- No ACK frames

Received Frames

- Frames received OK
- Beacons
- Frames with errors
- CRC errors

- ACK frames
- RTS Frames
- Clear-to-send (CTS) Frames
- No CTS frames
- Retried RTS frames
- Retried data frames

- Encryption errors
- Duplicate frames
- AP mismatches
- Data rate mismatches
- Authentication time-out
- Authentication rejects: the number of AP authentication failures received by the wireless network adapter
- Association time-out
- Association rejects: the number of access point authentication rejects received by the wireless network adapter
- Standard MIC OK
- Standard MIC errors
- CKIP MIC OK
- CKIP MIC errors

Chapter 4 Troubleshooting

This section provides solutions to problems usually encountered during the installation and operation of the USB adapter. Read the description below to diffuse your doubts.

What is the IEEE 802.11g standard?

802.11g is the latest IEEE standard for high-speed WLAN communications that provides up to 54Mbps data rate in the 2.4GHZ band. It has become the mainstream technology of current WLAN networks. It uses OFDM modulation to reach higher data transmission rate and backward compatible with 802.11b

What is the IEEE 802.11b standard?

The IEEE 802.11b WLAN standard subcommittee, which formulates a standard for the industry. The objective is to enable WLAN hardware from different manufacturers to interoperate.

What features does the IEEE 802.11 standard provide?

The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What is Ad-hoc?

An Ad-hoc mode is a wireless network type in which a group of computers equipped with wireless adapters are connected as an independent wireless LAN without any access point. All computers operating in this mode must be configured to share the same radio channel and SSID.

What is Infrastructure?

The difference between Infrastructure network and Ad-hoc network is that the former requires an Access point. The Infrastructure mode is appropriate for enterprise-scale wireless access to a central database or provides various wireless applications for mobile users.

What is BSS ID?

An Infrastructure network is called a Basic Service Set (BSS). All the wireless stations in a BSS must share the same BSS ID.

What is TKIP?

It is another encryption method to overcome the inherent weaknesses of WEP, a next generation of WEP. It adopts new algorithm (Michael) to generate 128/192-bit encryption keys and provides per-packet key mixing, a message integrity check and a re-keying mechanism.

What is AES?

AES (Advanced Encryption Standard) is a chip-based encryption method of new generation and has been incorporated into the newly-approved security standard 802.11i. It supports 128, 192 and 256-bit encryption key length and adopts Rijndael algorithm. It is widely believed it is impossible to crack AES.

What is DSSS? What is FHSS? And what are their differences?

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitters and receivers. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission**,** but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).